A CAHNERS PUBLICATION

FEBRUARY 15, 1989

DATAMATION

FOR MANAGERS OF INFORMATION TECHNOLOGY WORLDWIDE

OS Tug of War!

Unix and OS/2 Are Battling for Your Company's Desktops

TD642050 ( ) C63/ 89
STATISTICAL REFERENCE
CONGRESSIONAL INFO SERVI
4520 EAST WEST HWY
BETHESDA MD 20814

Also in This Issue:

The Virus Cure

Is Error-Free Software Possible?

Aiming IS at Business Targets

The Modem Protocol Duel

FEB 15, 1989

VOLUME 35
NUMBER 4

DATAMATION®

FOR MANAGERS OF INFORMATION TECHNOLOGY WORLDWIDE

Desktop Tug of War: OS/2 vs. Unix 18

BY BOB FRANCIS In its simplest form, the desktop decision facing IS managers boils down to two obvious choices—Unix or OS/2. Far more complicated are the issues that must be considered to make that deceptively simple decision. The prime determinant is the overall character of the application, which dictates other central issues such as power, complexity, and communications capabilities.

Unix Puts on a Friendly Face 21

Cover Photography by Jim Galante

DEPARTMENTS

Inside DATAMATION 4

Letters and Access 6
A raft of letters about computer science education.

Look Ahead 13
Computer Associates to pass $1 billion sales mark.

New Products 106
A CASE tool for developers who do Windows.

Planner 108

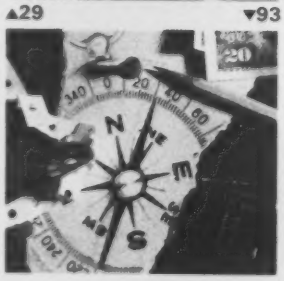
Opinion 108
Time for a change in the export controls on IT.

Career Opportunities 113

Company Index 120
A listing/locator of companies in this issue.

Ad Index 120

▲29 ▼93



SOFTWARE

SECURITY

The Virus Cure 29
BY JOHN McAFEE Some straight advice on how to prevent, recognize, and—if necessary—cure a viral attack on your computers.

The Recovery Period: Preventing Reinfection Is Key 35

LANGUAGES

The Future of SQL 45
BY DAVID BEECH In the second part of a rebuttal to E.F. Codd's articles "Fatal Flaws in SQL," a database researcher delineates ways that SQL can be improved.

PROGRAMMING

Is Error-Free Software Achievable? 53
BY EDWARD J. JOYCE The answer is "Yes," says prime NASA contract developer, IBM. And while $1,000 per line of code is prohibitively high for the average IS shop, some valuable lessons can be learned.

SYSTEMS

MAINFRAMES

Unix Goes Upscale 61
BY JEFF MOAD Large systems users and vendors opt for Unix because of innovations like high-performance multiprocessor architectures and SQL-based RDBMSs.

INTEGRATION

Frito Lays a New IS Bet 75
BY BOB FRANCIS Frito-Lay Inc.'s new decision support system will extend the valuable information from its much-lauded handheld computer sales network throughout the company, to its division managers on up to top decision-makers.

COMMUNICATIONS

MODEMS

The Dual-Protocol Modem Duel 81
BY ARIELLE EMMETT Last spring, the CCITT adopted dual protocols for the V.42 draft standard for error-correcting modems. Vendors say V.42 is expensive and time-consuming to implement. End users, meanwhile, appear confused or indifferent.

MANAGEMENT

REORGANIZATION

Aiming IS at Business Targets 93
BY THOMAS M. LODAHL and KAY LEWIS REDDITT Coalescing IS resources with multiplying business unit needs requires a significant investment of creative energy and, typically, more than one strategy. Here's a guide to integrating business and technology.

SECTORS

MANUFACTURING

Industry-Specific Advice, Solutions, Applications 104-1
EDITED BY LINDA RUNYAN A report on products, services, and methodologies for business unit managers in manufacturing businesses. Future editions will serve managers in the financial services and government sectors. (Not included in all issues.)

Living and Thriving at Technology's Edge

The leading edge of information technology is a destination that's neither easy to reach nor comfortable to occupy for very long. The travel costs can be extraordinarily expensive. And the rules of living there seem to change with every new advance in research, trend in business, or shift in policy. The rewards, however, are enormous, judging from the number of organizations that have embarked on journeys in search of technology that would give them sustainable leads over competitors—the edge, so to speak, over the other guy.

Many users, in fact, have already started down the road toward using desktop technology to its fullest advantage. Dallas Bureau Manager Bob Francis has been along for much of the ride in the past two years. One of the big forks facing those corporate travelers, he finds today, is the choice of advanced operating systems for the millions of PCs and workstations atop the desks and benches of their end users.

Photograph by Ben Weaver

PC RANGER FRANCIS sees organizational traits driving OS decisions.

In "Desktop Tug of War: OS/2 Versus Unix," p. 18, Francis measures the criteria by which users are evaluating the two OSs, including the the different memory requirements and interface qualities of Unix and OS/2. And he goes one step further, discovering through countless user interviews that it's the character of the organizations themselves that often dicates which path they follow. "When we decided to standardize on the Unix operating system," one IS exec tells Francis, "we had to examine not just what would save us the most money, but what kind of work each department did and what kind of work they might be doing in the future. So it wasn't an easy task."

The future in PC technology use is here today at a Pepsico Inc. division, Francis tells us in his companion article, "Frito Lays a New IS Bet," p. 75. Upon visiting chip maker Frito Lay Inc. in San Antonio, he realized that the Pepsi subsidiary was moving swiftly beyond its much heralded use of handheld computers into the realm of decision-support and executive-information systems built on an OS/2 chassis.

Unix itself is edging onto platforms besides workstations. San Francisco Bureau Manager Jeff Moad, who tracks large-scale systems developments for DATAMATION, reports that technological innovations such as new high-performance multiprocessor architectures and transaction-intensive RDBMSs for Unix systems are luring major users like the Internal Revenue Service to implement the OS on minicomputer and mainframe platforms. IS execs who believe such a move could give them an advantage should read "Unix Goes Upscale," p. 61.

Operating on the edge, of course, has its perils. One danger is that security is forgotten in the headlong rush to embrace the latest and greatest technology. Another is that the real computing needs of the organization are ignored in the pursuit. In "The Virus Cure, p. 29, John McAfee reminds us just how vulnerable distributed computing solutions have made many large corporations. Even more important, he offers some remedies for the security ills that can befall users in such environments. In "Aiming IS at Business Targets, p. 93, Thomas Lodahl and Kay Lewis Redditt argue convincingly that IS execs need to formally align their organization's business goals with their IS capabilities. If they don't, they risk going over the edge.

Tim Mead

—Tim Mead, Editor-in-Chief

DATAMATION®

Editor-in-Chief Tim Mead
Executive Editor David R. Brousell
Managing Editor Parker Hodges
Senior Editor Linda Runyan
International Editor Paul Tate
Art Director Robert L. Lascaro
Senior Writer Ralph E. Carlyle
Section Editors Theresa Barry, Marsha J. Fisher
Production Editor Catherine Kennedy
Production Assistant Suzanne P. White
Copy Chief Linda Bradford
Copy Editor Rene Matthews
Associate Art Director Anne Cooney
Assistant Art Director Sheri Marcus
Editorial Assistants Lauren Murphy (London), Karen J. Scher (New York)
Editorial Secretary Laura Giletti

Bureau Managers
Boston Gary McWilliams
Dallas Robert Francis
London Paul Tate
Los Angeles Tom McCusker
San Francisco Jeff Moad
San Jose Susan Kerr
Washington Willie Schatz

Foreign Correspondents
Eastern Europe David Hebditch (Leeds)
France James Etheridge (Paris)
Italy Janette Martin (Milan)

Contributing Editors Joseph Kelly, Fred Lamond, Hesh Wiener

Advisory Board Joseph Ferreira, John Imlay, Angeline Pantages, Russell Pipe, Carl Reynolds

Publishing Director Donald Fagan
Associate Publisher William Segallis
Marketing Com. Manager Sara Leiman
Production Manager Eric Jorgensen
Research Manager Laraine Donisi
Director of Production Robert Elder
Director of Art Department Barrie Stern
Circulation Manager Roxanne Wilson

EDITORIAL OFFICES
Headquarters: 249 W. 17 St., New York, NY 10011, (212)645-0067; telex 127703; fax (212) 242-6987. **New England:** 199 Wells Ave., Newton, MA 02159, (617) 964-3730. **Washington, D.C.:** 4451 Albemarle St. NW, Washington, DC 20016, (202) 966-7100. **Central:** 9330 LBJ Freeway, Suite 1060, Dallas, TX 75243, (214) 644-3683. **Western:** 12233 W. Olympic, Los Angeles, CA90064, (213) 826-5818; 582 Market St., Suite 1007, San Francisco, CA 94104, (415) 981-2595; 3031 Tisch Way, Suite 100, San Jose, CA 95128-2593, (408) 243-8838. **International:** 27 Paul St., London EC2A 4JU, England, (44-1) 628-7030; telex 914911; CPO Box 665, Tokyo, Japan, (81-3) 201-2335, fax 2135053.

DATAMATION (ISSN 0011-6963) Magazine is issued twice monthly on the 1st and 15th of every month by The Cahners Publishing Company, A Division of Reed Publishing USA, 275 Washington St., Newton, MA 02158-1630. William M. Platt, Chief Executive Officer; Terrence M. McDermott, President; Frank J. Sibley, Group Vice President; Jerry D. Neth, Vice President/Publishing Operations; J.J. Walsh, Financial Vice President/Magazine Division; Thomas J. Dellamaria, Vice President/Production and Manufacturing. Editorial and advertising offices, 249 W. 17th St., New York, NY 10011. Published at Woodstock, IL. Annual subscription rates: U.S. and possessions: $69; Canada: $98; Japan, Australia, New Zealand: $180 air freight; Europe: $157 air freight, $290 air mail. All other nations: $157 surface, $250 air mail. Reduced rate for U.S. public and school libraries: $47. Single copy: $10 in U.S. Sole agent for subscriptions in Japan is Maruzen Co. Ltd., 3-10 Nihonbashi, 2-Chome, Chuo-ku, Tokyo 103, J; sole agent for all other foreign subscriptions is J.B. Tratsart Ltd., 154 A Greenford Rd., Harrow, Middlesex HA1 3QT, England, (01) 422-8295 or 422-2456. No subscription agency is authorized by us to solicit or take orders for subscriptions. Circulation records are maintained at 44 Cook St., Denver, CO 80206. Phone (303) 388-4511. Second-class postage paid at Denver, CO 80206 and at additional mailing office. DATAMATION copyright 1988 by Reed Publishing USA, Saul Goldweitz, Chairman; Ronald G. Segel, President and Chief Executive Officer; Robert L. Krakoff, Executive Vice President. All rights reserved. DATAMATION is a registered trademark of Cahners Publishing Co. Reprints of articles are available; contact Frank Pruzina (312) 635-8800. Microfilm copies of DATAMATION may be obtained from University Microfilms, A Xerox Company, 300 N. Zeeb Rd., Ann Arbor, MI 48106. Printed by Graftek Press Inc. **All inquiries and requests for change of address should be accompanied by mailing label from latest issue of magazine.** Allow two months for change to be made. POSTMASTER: send address changes to DATAMATION, 44 Cook St., Denver, CO 80206.

THE VIRUS CURE

What was once considered science fiction is now reality as computer viruses creep into computer sites. Here's some advice on how to recognize and prevent viruses, and how to recover from infections.

BY JOHN McAFEE

In the summer of 1977, Thomas J. Ryan wrote and published a book that became an instant cult classic for computer hackers and technophiles. *The Adolescence of P-1* chronicled the fictional development of the world's first virus—a program that moved from computer to computer, taking control of the operating systems of 7,000 computers.

When this book first appeared, it was regarded as good science fiction. A mere 11 years later, a Cornell graduate student turned the experience into reality when he developed a program that ran amok: it jumped into the world's largest computer network and began taking control of the connected machines. The program was designed to both hide itself (fortunately the design had a bug) and defend itself against removal. It could also adapt to at least two radically different computer architectures. It spread like wildfire. The number of systems infected? 6,200.

Although Ryan did not apply the name "virus" to the subject of his book (Xerox developers in Rochester, N.Y., had been doing virus research for five years, but this use of the word was largely unknown to the general public), he anticipated the current state of affairs with accuracy.

Viruses have become a cold, harsh reality for a growing number of businesses, government agencies, and universities. The first seven months of 1988 produced over 300 major virus attacks, involving over 50,600 computers. Most were of unknown origin. Many involved substantial time and resources for removal, clean up, and restoration. Each was a surprise to the infected organizations.

The sudden appearance of the virus threat has caused vast amounts of misinformation and confusion to be generated. Standard terminology is in short supply. Prevention measures are incomplete and often conflicting. Recovery procedures are mostly seat-of-the-pants affairs. People are confused about what viruses are and how they spread, and snake-oil salesmen abound.

The confusion is not improved by conflicting opinions about the future of viruses. Some contend that it's a passing fancy that will take care of itself. Others feel we have seen only the tip of the iceberg.

Much of the confusion stems from limited and incomplete information. Many people have never seen a virus in action and are speculating about the effects and potential damage. Others have seen perhaps one or two examples of viruses, and extrapolate to the larger world of viruses from these small experiences. Even companies that fall prey to widespread in-

Illustration by Tim Grajek

fection, experiencing firsthand the devastating effects of viruses, often are unwilling to share their experiences with the public, or to provide guidance and counsel to other companies hit with similar infections. Less than 10% of the 300-plus organizations attacked by viruses this year were willing to publicly discuss their infections.

There is a general, and possibly warranted, feeling that a publicized virus infection will carry a social or commercial stigma that will harm a firm's image and marketing goals. Questions of lax security, disgruntled employees, damage to the organization, and impact on the company's products inevitably arise. The more a company's products use software as integrated components, the more this feeling prevails. Earlier this year, one large aerospace manufacturer threatened to sue a virus consultant who inadvertently slipped news of an infection to the press.

In spite of this cloak-and-dagger envi-

□ RESEARCHERS HAVE BEEN ABLE TO IDENTIFY OVER 30 DIFFERENT AND WIDELY DIVERSE STRAINS OF COMPUTER VIRUSES.

ronment, researchers have been able to identify over 30 different strains of viruses with widely diverse propagation mechanisms and destructive effects (see "The Six Most Common Computer Viruses"). Each of the strains has multiple varieties—a result of hackers' laziness: it is easier to modify someone else's virus than to build one's own from scratch. One Macintosh virus—nVIR—has over two dozen different varieties. As a result, hundreds of essentially different viruses are threading their way from system to system around the world.

What Are Computer Viruses?

Computer viruses are segments of self-replicating code that attach themselves to application programs or other executable system components. They attach themselves in a manner that allows them to gain control during some phase of the host's execution. Viruses can attach not only to boot sectors, operating system modules, and device drivers, but any application, such as a word processor, spreadsheet, or database system, is vulnerable.

Most viruses leave no external signs of their presence after infection. They infect the host in a manner that leaves the host functions unchanged. An infected pro-

The Six Most Common Computer Viruses

These are the culprits most often cited at infected computer sites.

Based on a study conducted by the Computer Virus Industry Association of its members, March 20, 1988, to Sept. 9, 1988.*

	Pakistani Brain	Scores
ORIGIN	Lahore, Pakistan, Jan. 1986. Developed by two brothers as as an experiment.	Electronic Data Systems, fall 1987.
HOST	IBM PCs and compatibles	Macintosh
CLASS	Boot sector infector	Generic application infector
DESCRIPTION	Replaces original boot sector. Moves original boot sector to another location. Adds seven sectors that contain remainder of virus. Flags all modified sectors as unusable to protect itself. Replicates onto all inserted bootable floppies.	Infects any application. Increases application size by 7,000 bytes. Seeks out new hosts at 3½-min. intervals. Creates notepad and scrapbook files in system folder. Creates invisible Scores and Desktop files. Looks for specific file names for destruction.
HOW SPREAD	Booting from unknown or shared diskettes. Infects through any access to an inserted diskette, e.g., listing directories, executing programs, through software reboot sequence.	Exchange of infected diskettes. Inserting diskette into infected system.
SYMPTOMS	Copyright @BRAIN Label displayed on infected diskettes. Reboot sequences are slowed down. Excessive floppy activity for simple tasks. Program crashes for some versions of DOS. Interrupt vectors modified.	Slowdown of system. Problems with printing. System crashes. File size increase. Notepad and Scrapbook icon modifications.
POTENTIAL DAMAGE	System crash can cause loss of data. Spreads quickly to all bootable disks.	Lost data due to system crashes.
PRECAUTIONS	Do not boot from unknown floppies. Boot only from hard disk, if one exists. Write-protect all bootable diskettes.	Do not exchange disks with others. Do not insert diskettes containing programs into others' systems. Do not execute programs from unknown sources.
RECOVERY	Shut down infected systems. Reboot from a clean, write-protected original boot diskette. List directories of all diskettes, look for @BRAIN label—if found, destroy the diskette or perform DOS SYS command to rewrite boot sector. Recreate volume serial label using any available utility. (This procedure will still leave 7 bad sectors with dead virus.)	Backup all data files. Erase the infected disk and all affected diskettes. Restore system files and applications from original masters. Restore data files.
NUMBER OF COMPUTERS INFECTED	18,158	14,207
NOTES	This virus will live through software reboot.	The Scores virus changes the small MAC icon for notepad and scrapbook into generic dog-eared page icons.

*A total of 61,795 infected computers were reported; from five to 816 were infected at each company. Other viruses, excluding the six in this table, infected 6,353 of the total reported. A total of 700,000 diskettes were infected.

Israeli Virus	nVIR	Alameda Virus	Lehigh
Hebrew University, Jerusalem, Dec. 1987.	Hamburg, Germany, summer 1987.	Merritt College, Oakland, Calif., spring 1988.	Lehigh University, Bethlehem, Pa., fall 1987.
IBM PCs and compatibles	Macintosh	IBM PCs and compatibles	IBM PCs and compatibles
Generic application infector	Generic application infector	Boot infector	System infector
Infects any .COM or .EXE program. Increases program size by approx. 1,800 bytes. Infected programs are modified to become memory-resident (TSRs). Programs are infected when they are executed in infected system. Floppy or hard disks can become infected.	The nVIR virus appears in many different varieties, each with its own characteristics. The publication of the source code for this virus is primarily responsible for the variations. The infection techniques are similar, however: places nVIR resource in system file; code resource in application. Once system is infected, all applications are infected.	Replaces original boot sector with itself. Stores original boot sector on first free sector. Infects through software reboot sequence. Does not flag original boot sector as unusual.	Infects COMMAND.COM file. Changes size by approx. 20 bytes. Changes creation date and time. Activates after four infections. Destroys all system data.
Transfer of infected programs on floppies. Inserting floppies into infected computers.	Sharing of diskettes, inserting diskette into infected system. Executing of infected program.	Booting from a diskette of unknown origin. Inserting a clean boot diskette into an infected system.	Sharing infected diskettes. Inserting a clean diskette into an infected system.
General slowdown of the system. Programs disappear on Friday the 13th. .EXE files continue to grow in size until too large to execute. Available system memory decreases.	nVIR symptoms vary greatly due to the large number of varieties. Some symptoms are: system crashes; a "beep" when an application is opened; with MacinTalk installed, "don't panic" message is heard; files disappear.	Slow boot sequences. System crashes. Lost data.	Change in size of COMMAND.COM. Loss of all system data.
Some versions destroy all data on the hard disk. Stored programs will disappear.	Loss of data and programs. Frequent system crashes.	Loss of data.	Loss of all data on hard disk.
Do not execute programs from unknown sources. Do not exchange diskettes containing executable code with others. Monitor memory allocation and program file sizes.	Do not share diskettes with others. Quarantine infected systems. Do not work with original master diskettes.	Boot only from one write-protected floppy. Do not boot hard-disk systems from a floppy. Do not insert boot diskettes into another's system.	Do not transfer application programs on a system diskette. Do not insert any system diskette into another's computer. Monitor COMMAND.COM file for date/size changes.
Power down the system. Boot from a write-protected original boot diskette. Delete all executable programs on hard disk and affected floppies. Replace programs using original distribution diskettes.	Backup data files. Erase infected disks. Restore programs from original master copies (write-protected). Restore data files.	Power down the system. Boot from a write-protected original master diskette. Execute the DOS SYS command to replace boot sectors of diskettes.	Power down the system. Reboot from original write-protected system master. Delete COMMAND.COM from hard disk and all affected floppies. Restore COMMAND.COM from original master.
3,575	11,066	3,482	4,943
There was a bug in the virus that caused .EXE files to become infected over and over again. This made the .EXE file size increase until the programs could no longer fit into memory. This problem has been removed in later versions by unknown hackers.	nVIR is particularly virulent and can infect all programs within an infected system in a matter of minutes.	The Alameda virus, unlike the Pakistani Brain, does not protect the original boot sector after infection. The original instructions may be overwritten by accident. Boot failure then occurs.	The Lehigh virus has a very short activation period (four infections). Because of this, the chances of detection before data destruction is slim.

On February 15, 1988, IBM announced its most significant storage management advance in more than 20 years, DFSMS.™ This new software can manage vast quantities of information on disks and other storage devices, provide for more effective use of IBM storage hardware and improve end-user service—all automatically.

This means programmers can now spend less time controlling and more time creating.

IBM®

© Copyright IBM Corporation 1989. DFSMS is a trademark of the IBM Corporation. IBM is a registered trademark of the IBM Corporation.

On February 15, 1988, IBM announced Enterprise Systems Architecture/370,™ the industry's most advanced systems architecture. Also announced was a new operating system, MVS/ESA.™

MVS/ESA enables new approaches in application design because it gives users of IBM's most powerful processors 16 trillion characters of virtual storage.

8,000 times more than they had before.

IBM®

© Copyright IBM Corporation 1989. Enterprise Systems Architecture/370 and MVS/ESA are trademarks of the IBM Corporation. IBM is a registered trademark of the IBM Corporation.

gram may operate normally for months, or even years, without giving any signs of the infection. During this time the virus quietly replicates onto other programs within the system, and onto floppies inserted into the computer.

After an indeterminate replication period, the virus activates. This involves some type of overt system disturbance. It may be as innocuous as the display of a message or some unusual graphics, or it may involve partial or total destruction of stored data. The particular manifestation is based on an internal algorithm, which may be determined by the length of time the virus has been in the system, or by the number of programs or floppy diskettes already infected by the virus. Some viruses activate based on the number of times the infected host program has been executed. Others activate on a given day and time, such as noon on any Friday the 13th. Regardless of the algorithm used, activation usually means bad news.

Viruses can be grouped into three categories: boot infectors, system infectors, and generic application infectors.

Boot infectors attach themselves to the boot sectors of floppies and hard disks. They gain control of the system when it is initially booted and remain in control at all times. They monitor all system activity by trapping software interrupts, and watch for the insertion of new floppies into the drives. When a diskette is inserted and accessed for the first time, the virus transfers itself to sector 0 of the floppy, then it infects the next system booted from that floppy. Booting from an infected floppy is the only way this group of viruses can infect a new machine.

System infectors attach themselves to at least one operating system module or system device driver. They can infect command interpreters, system I/O routines, or special-purpose drivers for attached hardware. They gain control after system boot—during operating system initialization—and stay active in the system at all times. They watch for the insertion of system diskettes into one of the floppy drives. When this occurs, the virus replicates onto the system files.

Generic application infectors are able to infect any application program. They gain control when an infected application is executed, and they scan the system looking for additional hosts on hard disks and floppies. When found, they attach to the new hosts. After the virus scans and infects, it generally passes control back to the application program. Generic application infectors are the most widespread of all viruses.

Viruses have been transmitted across local area networks, through access to bulletin boards, and through a number of remote computer-to-computer communication links. In the personal computer arena, however, the overwhelming majority of infections occur because of program or data sharing through infected diskettes.

Boot infector viruses, for example, can infect in no other way. They require that a diskette be the transfer medium from machine to machine. System infectors also prefer diskette transfer, and they wait for system diskettes to be inserted into an infected machine to continue the replication process.

Diskette sharing and transfer are widespread practices among personal computer users. Even in large corporate environments we frequently find PC users sharing machines and resources. A machine with the only high-quality laser

□ AN INFECTED PROGRAM MAY OPERATE NORMALLY FOR YEARS, WITHOUT GIVING ANY SIGNS OF THE INFECTION.

printer in the department, for example, may frequently be borrowed by other users in the department. These users will typically bring their own diskettes with files to be printed. If a diskette happens to be infected, then the machine with the laser printer becomes infected, and thereafter, every user will take away an infected diskette. The virus thus spreads rapidly throughout the department.

What mechanisms do viruses use to attach themselves to other programs? Viruses infect in one of two ways: they attach to an existing piece of code, or they entirely replace a piece of code. Certain boot-sector viruses use the latter approach. They replace the entire boot sector with a copy of themselves. In effect, they become the new system boot program. Most viruses, however, choose to attach themselves to an existing program. This approach alleviates the problem of the virus having to duplicate the functions of the program it replaces.

How Viruses Are Spread

A virus attaches to a program either by binding itself externally to the program or by implanting itself inside the program. If it attaches externally, then the program size usually changes, and the virus risks detection from a visual inspection of di-

On March 15, 1988, IBM expanded the line of IBM AIX™ operating systems to include support of our most powerful processors.

This will provide advanced, consistent AIX function across a full range of IBM products, from the Personal System/2® and mid-range computers, to the largest 3090™ systems, offering the broadest range of products based on UNIX operating systems in the industry.

Now users have a lot more in common.

IBM®

© Copyright IBM Corporation 1989. AIX and 3090 are trademarks of the IBM Corporation. Personal System/2 is a registered trademark of the IBM Corporation. IBM is a registered trademark of the IBM Corporation. UNIX is a trademark of the AT&T Corporation.

On March 16, 1988, IBM researchers tested the world's fastest silicon circuits, made from wiring that is 1,000 times thinner than a human hair.

Capable of switching on or off 75 billion times a second, such new circuits may promise desktop computers as powerful as today's largest mainframes.

IBM®

© Copyright IBM Corporation 1989. IBM is a registered trademark of the IBM Corporation.

On April 19, 1988, IBM introduced an advanced version of its premier relational DATABASE 2 (DB2™), providing substantial performance improvements over the previous release.

IBM's new DB2 Version 2 offers significant new functions such as referential integrity, which allows customers to maintain data relationships without the need for complex programming.

Responding to customer requests, these changes increase database performance and programming productivity.

IBM

© Copyright IBM Corporation 1989. DB2 is a trademark of the IBM Corporation. IBM is a registered trademark of the IBM Corporation.

On May 13, 1988, IBM unveiled its plans for the Advanced Automation System (AAS). This system is designed to help the Federal Aviation Administration's air traffic control system safely handle the estimated 60 percent increase in U.S. air traffic by the 21st century.

Thank you for flying IBM.

IBM

© Copyright IBM Corporation 1989. IBM is a registered trademark of the IBM Corporation.

rectory listings or other external observations of the program. If the virus chooses to insert itself within its host, then it must find hosts with enough internal free space to hold the virus. Most programs do not have sufficient free space. Thus the virus has a more limited number of receptive hosts and will spread more slowly.

Evidence suggests that virus designers have weighed the above considerations and opted for external attachment. These viruses attach by replacing the initial instructions of the host program with new instructions that branch to the main body of virus code. This code is usually tacked on to the end of the host application. After execution of the virus, the original program instructions are restored and control is passed to the host.

□ THE PROGRAM SIZE USUALLY CHANGES IF A VIRUS ATTACHES EXTERNALLY, ALLOWING VISUAL DETECTION.

There are ways to limit exposure to virus infection. Risk reduction can be divided into two areas: antiviral tools and safe user practices.

Many virus infections can be easily prevented with the appropriate tools. A number of software products are available that provide varying degrees of protection, and should be considered as valid tools in antiviral efforts.

Antiviral Programs

Each class of virus uses a different mechanism for infection, and each individual strain uses its own unique methods for activating and corrupting the system's data. A cursory review of a number of disassembled viruses would lead one to believe that no technique could possibly catch all existing viruses, let alone new ones not yet sampled. This assumption, however, would be wrong. The situation is neither as hopeless nor as complex as it first appears.

To understand how viruses can be effectively neutralized, we must first appreciate some fundamental limitations of viruses—their weak points. Also, we need to extract features that are common to all viruses and turn these universal features to advantage. This may seem rather daunting, but in fact it has already been accomplished, and the results have been embodied successfully in a number of antiviral products.

The first and most important limitation that all viruses possess is that their host

The Recovery Period: Preventing Reinfection Is Key

The main problem in recovering from a virus is not the loss of data, but the near certainty of reinfection if the proper procedures are not followed. Nine out of 10 installations that get infected experience a relapse within a week of "cleaning out" the virus. The causes of these reappearances can be traced to two things. First, many viruses do not go away after a warm boot. The Pakistani Brain is such a virus. Second, viruses initially infect fixed disk systems by way of a floppy diskette. After infection, every floppy that has been placed in the system is also likely to be infected.

When an infection is detected, follow these procedures:

1. Determine the extent of infection. If the virus has not attacked any fixed disks, go to step 12. If the virus has infected the boot sector only, see the addendum.
2. Power down the infected system.
3. Retrieve the original system diskette from the distribution package. Write-protect it. Place it in the floppy boot drive and power up the system.
4. Ensure that the system has booted properly.
5. Back up all nonexecutable files from all directories onto newly formatted floppy diskettes or to a tape backup unit. If backing up to another fixed disk, ensure that the disk has not been infected. (If there are any doubts, assume that it is). Do not use the backup utility on the fixed disk. Use a utility from the original package.

(Note: At no point in these procedures should you execute *any* program from the infected fixed disk!)

6. List all batch files on the infected disk. If any line within any of the batch files seems unusual or unfamiliar, do not back up. Otherwise, include the batch files with the backup.
7. Perform a low-level format of the infected disk.
8. Restore the operating system to the fixed disk.
9. Restructure your directories.
10. Replace all executable programs from the original distribution packages.
11. Restore the files that had been backed up.
12. Locate all floppy diskettes that may have been inserted in the infected system within the past two years. (It sounds extreme, but if this and subsequent steps are not followed, you can be guaranteed reinfection within a short period of time).
13. At your discretion, either destroy all such floppy diskettes or proceed with the following steps.
14. Back up all nonexecutable files onto newly formatted floppy diskettes.
15. Format the suspect diskettes.

Addendum

If the virus is a boot sector infector, the recovery process is somewhat simplified. Since boot infectors do not infect executable programs, they can be removed by replacing the bootable system on the affected drive. The procedures are:

- Power down the affected system.
- Boot from the original write-protected system diskette.
- Replace the operating system and boot sector on all affected devices.

The above procedures will leave the virus intact on the additional bad sectors originally allocated by the virus, but these viral segments will be deactivated.

targets must be executable segments of the computer system. That means they can only infect other programs, whether boot segment programs, operating system elements, or applications. They cannot effectively infect data files, spreadsheets, tabular information, or any raw data elements within the system. This may seem like small comfort, but in fact, as will shortly be demonstrated, it is a limitation that can be used to great advantage in the war against viruses.

The second limitation is that any infection, no matter how sophisticated, must change the infected segment of the system in some fashion. The virus either entirely replaces a segment of the system or it modifies the existing segment. If it attaches to an existing program, then it changes the beginning, the end, or some part of the middle of the program. If it hides in vacant areas of the disk, then those areas suddenly become no longer vacant, and are modified. If the virus stores the original boot sector in some unobtrusive place, then the move itself changes the system. The rule is this: any infection leaves some residual trace.

The third weakness is that if the virus is to live and multiply, then its program code must be run, or executed, at some point. That is, the virus must place itself in a position to get control of the computer at least once after the initial infection—otherwise the virus will never be able to replicate or activate.

On June 2, 1988, IBM introduced seven new desktop products, including the IBM Personal System/2® (PS/2®) Model 70 386.

The Model 70 386 features high-speed memory and IBM's Micro Channel™ architecture, which improves data integrity and allows users to run large, multiple programs more reliably and efficiently.

In fact, by the end of 1988, over 600 Micro Channel add-in boards were available to enhance the power of the PS/2.

That's a lot of desktop options for almost any desk.

IBM®

© Copyright IBM Corporation 1989. IBM, Personal System/2 and PS/2 are registered trademarks and Micro Channel is a trademark of the IBM Corporation.

On June 21, 1988, IBM announced the Application System/400,™ the largest product introduction in IBM's history. This powerful, easy-to-use computer system is designed to grow as fast as customers' needs and provide consistency in applications, and is IBM's first product family to conform to IBM's Systems Application Architecture.™

So even though you can't predict the future, you can now adjust to the future easily and quickly.

Say good-bye to future shock.

IBM

© Copyright IBM Corporation 1988. Application System/400 and Systems Application Architecture are trademarks of the IBM Corporation. IBM is a registered trademark of the IBM Corporation.

On June 28, 1988, IBM introduced ImagePlus,™ a new image processing system that will help businesses that process large amounts of paperwork reduce costs, improve customer service and design more competitive products and services. This system will improve the way a business handles the paper it receives from, and sends to, its customers.

Businesses using ImagePlus will be able to take an "electronic picture" of customer letters, sketches and even photographs and move them instantly through the business for processing.

Can you picture that!

IBM

© Copyright IBM Corporation 1989. ImagePlus is a trademark of the IBM Corporation. IBM is a registered trademark of the IBM Corporation.

This implies that the virus cannot just attach itself to programs at random. It must know something about the general structure of host programs and attach itself so that it executes whenever the host program is executed. This need to position itself (or at least parts of itself) in specific areas of the host program is a limitation that can also be used to advantage by antiviral systems.

In sum, viruses must infect specific types of data (programs), they must position themselves (at least partially) in limited and specific areas of the programs, and the act of infection invariably causes some change in the system. These points may not sound like much to go on, but when they are viewed in the context of the average computing environment, a great deal can be made of them.

A description of how the various types of antiviral systems take advantage, each in their own way, of one or more of the above weaknesses, will explain how these three points can be leveraged.

Three Types of Antiviral Programs

There are almost as many approaches to developing antiviral software as there are types of viruses. On analysis, however, the antiviral programs fall naturally into three different categories:

- Infection prevention products. These products stop generic viral replication processes and they prevent viruses from initially infecting the system.[7] They are usually not specific to individual viruses, but protect against all classes of viruses.
- Infection detection products. These products detect an infection soon after the infection has occurred. They generally identify the specific area of the system that has become infected. Like infection prevention products, they identify generic infections rather than individual viruses.
- Infection identification products. These products identify specific viral strains on systems that are already infected, and usually remove the virus—returning the system to its state prior to infection.

Infection prevention programs remain resident in a computer's memory at all times. They monitor all system activity, watching for characteristic signs of viral replication. These programs filter the file accesses (reads and writes) attempted by other programs. They monitor the programs that load into and out of memory. They check all requests for operating system services. They keep watch over system tables and system control structures. Virtually every aspect of the system's activities is monitored and checked as it occurs.

These antiviral programs all wait for the same event: an indication that a virus is attempting to infiltrate the system, which nearly always is indicated by an attempted access to one of the executable programs in the computer—the boot segment, the operating system, or an application program. When such an access is attempted, the program freezes the system (before the virus can complete replication) and flashes a warning message to the system user. The virus can then be harmlessly removed.

How, though, does the antiviral program distinguish between a virus trying to access a program and any other harmless function trying to do the same thing? How is the virus's access different from that of a word processor or a database program? The answer is that in the normal course of events a word processor would never attempt to access or write to another program. Neither would a database system, nor a spreadsheet program, nor a graphics package. In fact, normal modifications of, or accesses to, executable segments of a computer are extremely rare. Such accesses would take place only if the program in question were being replaced by a newer version, or was being initially loaded into the computer.

At least this is the theory. In practice, however, there are a number of normal computer system functions that can cause these types of antiviral programs to believe that a virus is present. When this occurs, a false alarm is sounded. One measure of the quality of such programs is the frequency of false alarms. Well-designed, sophisticated programs will present few. Poorly designed programs may cause so many that the program becomes useless.

Prevention programs can also be fooled by the viruses themselves. Some viruses use infection mechanisms that are specifically designed to avoid this kind of detection. Such viruses use access techniques that are difficult to monitor or prevent. These techniques involve writing directly to the hardware that controls the storage devices, or using I/O calls that bypass the antiviral checking function. These viruses are more difficult and time-consuming to implement but they can be, and are being, created.

A final weakness of prevention programs is that they cannot keep boot segment infections from occurring. This is because boot segment infections occur as the system is powered up or rebooted. At that point, the infection prevention program has not yet been loaded, and is therefore powerless. This is a fundamental architectural drawback of this class of protection device, and technical advances are not likely to overcome this limitation.

Infection Detection Programs

In spite of the above three problem areas, infection prevention programs can provide a statistical margin of safety for the average computer user. It may be better to catch and prevent, say, 86% of all infections than not to catch any at all.

□ VIRTUALLY EVERY ASPECT OF A SYSTEM'S ACTIVITIES IS MONITORED BY ANTIVIRAL PROGRAMS.

Infection detection programs work on the principle that virus infections can be detected after they occur by locating the infection traces. These traces are the modifications or changes in the system made by the viruses during the infection process. These programs are generally more reliable than infection prevention programs, and they are effective against all classes of viruses.

Infection detection programs work in one of two ways: through vaccination or through a snapshot technique.

Vaccination works by modifying the programs in the computer to include a self-test mechanism within each program. The test mechanism uses a checksum or other mathematical or algorithmic technique to determine if the sequence of instructions within the program has been altered. This self-test executes each time the program runs, and it checks the program to see if any changes have been made since the last time the program was executed. If the program is in any way different, a virus infection is assumed, and a warning to the user is displayed.

Vaccination has a number of major drawbacks. The most important is that many critical programs in the computer, including the boot segment, are difficult—often impossible—to effectively vaccinate. Remember that boot segment viruses generally replace the boot segment in its entirety. Consequently, the vaccinated boot sector never gets a chance

On July 19, 1988, IBM introduced Disk Operating System (DOS) software, version 4.0, with an easy-to-use shell and expanded memory functions.

In fact, the new DOS 4.0 contains more than 30 new and enhanced functions that can be used across our entire personal computer line.

IBM

© Copyright IBM Corporation 1989. IBM is a registered trademark of the IBM Corporation.

On July 19, 1988, IBM announced three new RISC Technology systems, increasing RT* System performance by up to 25 percent, furthering IBM's commitment to customers using high-performance UNIX operating systems.

Users of the larger RT models can now have 1,176,000,000 more bytes of disk storage available than they had the day before.

IBM

© Copyright IBM Corporation 1989. RT and IBM are registered trademarks of the IBM Corporation. UNIX is a registered trademark of the AT&T Corporation.

On July 26, 1988, IBM introduced the world's most powerful general-purpose processor.

The Enterprise System/3090™ Model 600S with MVS/ESA™ software increases application processing power by as much as 56 percent, and for numerically intensive applications such as weather forecasting, there is a 40 percent increase in computing performance.

But even though it can help make weather reports more accurate, it still can't change the weather.

IBM

© Copyright IBM Corporation 1989. Enterprise System/3090 and MVS/ESA are trademarks of the IBM Corporation. IBM is a registered trademark of the IBM Corporation.

to execute after the infection, and therefore can never alert the user. Even if it could be executed, the self-test would not identify any problems, since the virus only moved the boot segment and did not otherwise change it.

The second problem with vaccination is that no matter how effective the self-test algorithm may be, a virus that infects a vaccinated program invariably gains control *before* the self-test mechanism executes. From this vantage point, the virus can still replicate, possibly activate, and even (with sophisticated viruses) disable the self-test mechanism before it can execute.

Despite these drawbacks, the vaccination form of viral detection products can still provide a degree of protection. As with infection prevention products, it is better to partially protect than not to protect at all.

Perhaps the most effective form of protection available today is provided by infection detection products that use an efficient snapshot technique. Snapshot programs work by logging all critical information in the system at the time of initial installation. Thereafter, a check routine is periodically run to compare the current state of the system with the original snapshot. If traces of infection are detected, the affected area of the computer is identified and the user is notified.

Snapshot programs have the advantage that all parts of the system can be checked, cross-checked, and compared at the same time. Because of this, boot sector infections, operating system viruses, and generic viruses can all be detected. A second advantage is that the snapshot file and the compare program can be kept off-line, that is, outside of the computer, inviolable.

Snapshot techniques have been very successful in identifying virus infections soon after they occur. One possible drawback with some of these programs, however, is that the verification techniques (checksums or other math algorithms) can take a considerable time to check an entire system. Some newer products do employ innovative techniques to speed up this process. A few products, for example, use a technique called "branch address maps" to check executable programs for traces of infection. Such products are able to verify entire computer systems with hundreds of programs, including the boot segment and all operating system files, in a matter of seconds.

The check routines used by snapshot programs can be run at any time to see if a virus has invaded the computer. Most pro-

grams, however, also provide an automatic check function. This function is executed periodically, for example, each time the computer is turned on or rebooted. If an infection is identified, these snapshot programs will zero in on the specific program or area of the system that has been invaded. Removal is usually a straightforward process for most viruses if identified early enough, and the process is normally documented in the product's manual.

These products are, to date, the most effective in providing protection against infections. They do have one drawback, however. There is a small risk that the virus will activate before the detection program can be run to check for it. For example, you may get infected the morning of Friday the 13th by a virus that activates on Friday the 13th. In this case, the check program would not be executed until the next time you reboot or power the computer on—probably the following day. In the interim, the virus would have activated and wreaked its havoc. The probability of such occurrences, however, is low.

Infection Identification Programs

What if your system is already infected, and the virus has spread to every conceivable part of the computer? What if it has even begun to activate, destroying a good part of your data and infecting all 200 of your floppy disks? It's a little too late for prevention, and detection is all too obvious.

When this happens, the third category of antiviral products comes into play. These products seek out specific strains of viruses in every corner of your system. When they find them, they deactivate them or completely remove them.

These products work by looking for specific characteristics of individual viral strains. They may scan the system for a particular segment of virus code, or look for virus labels or copyright flags. They may look for specific system interrupt modifications that are unique to the virus, or for specific file names or key data in fixed disk addresses. When any of these flags are found, the virus is tracked down and eradicated.

On the surface, such programs appear to be panaceas. They all have one extremely limiting factor, however—their designers need a working sample of the virus they are attacking before they can come up with an antidote. This means that a virus must first be identified, isolated, captured, and disassembled (a process that may take months) before the designer can get down to work. Next, the design has to be implemented, and then the finished product must be packaged and marketed. The complete cycle may take one or two years from the time the virus is first placed into circulation.

Thus, infection identification products will always be behind the power curve of the antiviral war. But a program that performs the task of cleaning out the virus from thousands of infected disks is many times faster, cheaper, and more effective than any manual method of recovery from infection, and can be invaluable to large organizations.

□ SNAPSHOT TECHNIQUES CAN SUCCEED IN IDENTIFYING VIRUS INFECTIONS SOON AFTER THEY OCCUR.

Safe User Practices

The implementation of appropriate practices for computer users within an organization is equally as important as the use of antiviral programs. A few simple procedures can greatly reduce the exposure to virus infections (for tips on recovery once infected, see "The Recovery Period: Preventing Reinfection Is Key").

1. First and foremost, never boot from any floppy other than the original write-protected diskette from the original distribution package! Most of the boot sector infector viruses can infect your system *only* if you boot from an infected floppy diskette. Booting from borrowed, unknown, or multiple diskettes greatly increases the opportunity for infection.
2. One and only one boot diskette should be assigned to each and every floppy-based PC (systems without a fixed disk), and that diskette should be *clearly* labeled as the boot diskette for that system.
3. If you have a system with a fixed disk, *never* boot from a floppy drive. The only exceptions to this involve recovering from a viral infection.
4. Treat public domain and shareware software with caution. If possible, limit use of such programs to systems without fixed disks. If you do use them on fixed disks, allocate separate subdirectories for

On August 16, 1988, IBM announced new and enhanced artificial intelligence software that is designed to capture the knowledge of your most experienced employee and make it available to everyone. So even inexperienced employees can make the right business decisions.

Now everyone can be an expert.

IBM

© Copyright IBM Corporation 1989. IBM is a registered trademark of the IBM Corporation.

With the introduction of five new software products on September 20, 1988, IBM became one of the first U.S. manufacturers to incorporate into their machines systems network programs based on international standards.

Taking advantage of Open System Interconnection (OSI), a set of international standards and protocols, IBM computers are now "multi-lingual": they can talk to networks of IBM machines or any other manufacturer's.

And that's got everybody talking.

IBM

© Copyright IBM Corporation 1989. IBM is a registered trademark of the IBM Corporation.

On October 12, 1988, IBM entered into an agreement with Steve Jobs and NeXT that allows IBM to bring the NeXT advanced graphical interface to IBM's AIX™ workstations.

Who knows what's next?

IBM

© Copyright IBM Corporation 1989. AIX is a trademark and Personal System/2 is a registered trademark of the IBM Corporation. IBM is a registered trademark of the IBM Corporation. NeXT is a trademark of NeXT, Inc.

the public domain programs. This will reduce the chances of exposure since some viruses limit their replication activities to the current subdirectory.

5. Create meaningful volume labels on all fixed and floppy disks at format time. Develop a habit of checking volume labels each time a Dir command is executed. Keep a lookout for changes in the volume labels.

6. Watch for changes in the pattern of your system's activities. Do program loads take longer than normal? Do disk accesses seem excessive for simple tasks? Do unusual error messages occur with regularity? Do access lights on any of the system devices turn on when there should be no activity on that device? Do you have less system memory available than usual? Do programs or files disappear mysteriously? Do you suddenly notice a reduction in available disk space? Any of these signs can be indicative of viral infections.

7. If you are in a corporate or multisystem environment, minimize the exchange of

□ WATCH FOR CHANGES IN THE PATTERN OF YOUR SYSTEM'S ACTIVITIES.

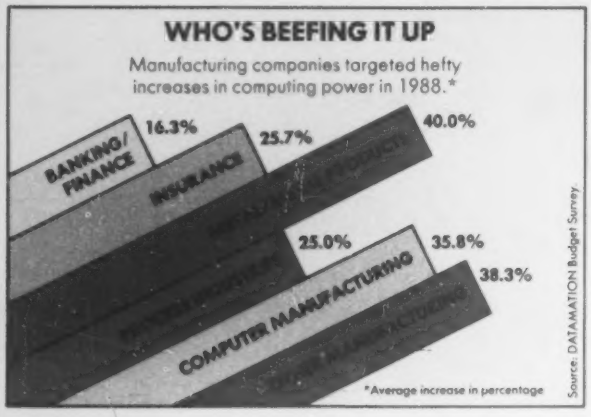
executable code between systems wherever feasible. When using resources on someone else's PC (a laser printer, for example), transfer the necessary data on a diskette that contains no executable code. Also, do not use diskettes that are bootable or that contain system files.

8. If operating in a network environment, do not place public domain or shareware programs in a common file server directory that could be accessible to any other PC on the network.

9. If operating in a network environment, do not use the file server node as a workstation. Allow no one other than the system administrator to use the file server node.

10. If using 3270 emulators connected to mainframe systems, keep all 3270 emulation software together in a separate subdirectory and do not include *any* executable code in the subdirectory that is not part of the emulator suite. If possible, limit such terminals to 3270 emulation only, and remove all other software from the disk. 3270 emulators are the major gateways through which viruses jump from PCs to mainframes. □

John McAfee is an industry consultant and president of Interpath Corp., Santa Clara.



JIT Arrives On Time At NEC Plant

The just-in-time (JIT) manufacturing methods that migrated from Tokyo to the States and beyond will be arriving not a minute too soon at NEC Information Syst.,as' plant in Boxborough, Mass. JIT tactics will be increasingly deployed at the plant as the company shifts from imported to U.S. parts in the production of dot matrix printers and Powermate PCs. The shift, which started last summer, should help the Japanese manufacturer reach its goal of boosting local content in those wares from 5% to 40%.

The JIT parameters and criteria that establish precise, narrow delivery windows for supplies to be received will be fed through the Honeywell Manufacturing System (an MRP II package) into NEC's Honeywell DPS 8/49 main frame. The first U.S. supplier on the JIT list will be NEC's printed circuit board subcontractor. The domestic-part procurement strategy made possible by JIT is mandatory if NEC is to be a long-term competitor in the American computer market, where product life cycles are accelerating at a fast clip.

"You must build a product closer to the market to be able to react more quickly," explains Herb Spivak, vp of manufacturing at the Boxborough facility. "If you're ordering materials for yesterday's product, you're in trouble."

There are economic considerations as well. "The Japanese have the technology," he notes, "but they can't fight against the economics of their strong currency."

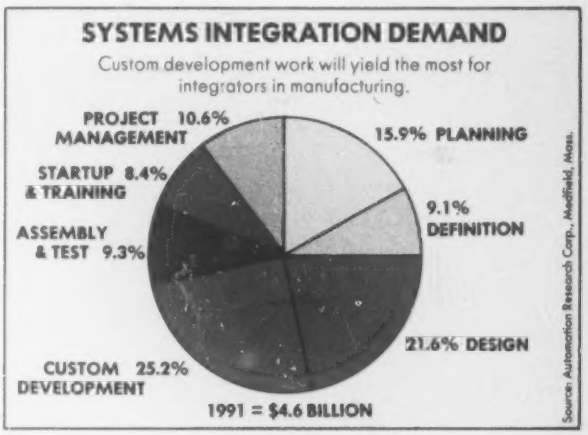
The Japanese also place "a heavier emphasis on testing and quality control," according to Spivak. "Every week, we send to NEC in Japan very detailed reports of our test results and information on any defects or assembly errors found," he notes. If there's a change or a problem develops, "they'll ask for more data. They're very attentive to the final quality of the products coming off their assembly lines." ◀

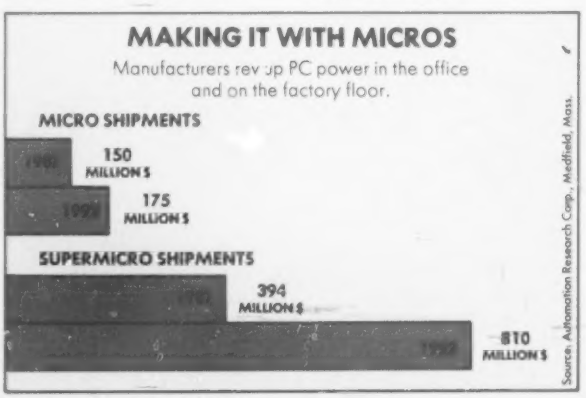
PCs Make Mark in Plants

More and more manufacturers are making and moving their products with the help of micros. Automation Research Corp. of Medfield, Mass., predicts that for U.S. industrial applications the value of microcomputer shipments—from low-end machines through dedicated workstations—will skyrocket in the next few years.

The growth at the high end of the small systems spectrum is much more spectacular than at the lower end. ARC expects that the value of shipments of 32-bit PCs will more than double to $810 million by 1992 from $394 million in 1987; 16-bit units used in industrial settings will grow slightly to $175 million from $150 million during that time. Workstations, which are not included in this ARC tally, will be the real workhorses on the factory floor. The research house forecasts that between 1987 and 1992 the value of workstation wares shipped for industrial automation chores will be over $145 million, up from $63 million.

Design work—one of the more complex industrial automation chores—is also getting a big boost from small machines. A survey conducted by the *Anderson Report* found that PCs were the most popular CAD tools among its sample, which was skewed toward larger companies. Out of a survey total of 13,588 CAD seats, 66% were PCs and 22% were workstations. The most frequent applications were two-dimensional and three-dimensional CAD, followed by solid modeling and electronics. ◀


SYSTEMS INTEGRATION DEMAND
Custom development work will yield the most for integrators in manufacturing.
PROJECT MANAGEMENT 10.6%
15.9% PLANNING
STARTUP & TRAINING 8.4%
9.1% DEFINITION
ASSEMBLY & TEST 9.3%
21.6% DESIGN
CUSTOM DEVELOPMENT 25.2%
1991 = $4.6 BILLION
Source: Automation Research Corp., Medfield, Mass.


MAKING IT WITH MICROS
Manufacturers rev up PC power in the office and on the factory floor.
MICRO SHIPMENTS
150 MILLION $
175 MILLION $
SUPERMICRO SHIPMENTS
394 MILLION $
810 MILLION $
Source: Automation Research Corp., Medfield, Mass.

Software Speeds Up VW

Next month, West German automaker Volkswagen will be cruising in the fast lane with a new system designed to speed up the purchase of materials needed in car construction. The software being developed for the $31.6 billion car company by French firm Cap Gemini Sogeti will churn out computer-aided estimation data and information pertaining to the frequency of specifications and options such as auto color and transmission type.

Estimates of the need for various option combinations, calculated over several months, will enable Volkswagen to order and stock just the amount of parts it needs, thus reducing its inventory-carrying costs, according to the company. The $850,000 system, dubbed Prisma, will be up and running full speed ahead in March on an IBM 3090 mainframe operating under MVS and IMS. ◀

Charts by Catherine Francis